FROM THE EDITORS OF

COMPUTERWORLD

VOLUME 3, NUMBER 5

MAY 25, 1998

Intranets

A MONTHLY LOOK AT WEB DEVELOPMENTS BEHIND THE FIREWALL

DIRECTORY SERVICES

Unraveling the Riddle

NationsBank's Brian Ehorn recognizes LDAP's challenges, but is pushing ahead

By Suruchi Mohan

LDAP could simplify intranet administration, but at what cost?

Brian Ehorn faces a tough task. The manager of global finance Web services at NationsBank in Chicago wants his far-flung organization to have faster access to key bank and group services data. So he's creating tools to allow remote employees — and even authorized bank customers — to see this data as if they were attached to the corporate intranet.

Similarly, Federal Express Corp.'s Jim Candler, vice president of personnel systems, is convinced that enabling employees to see and update their personal human resources data is

Continued from page 1

a good thing. So Candler and his HR team have created an environment that lets employees inside a firewall authenticate themselves and query and alter their own data through a special FedEx browser.

For Jeremy King at Bay Networks, Inc. in Santa Clara, Calif., the challenge goes beyond access and authentication. For the project manager of this leading internetworking company, consolidating security applications and maintaining users and groups on the corporate intranet is proving to be more than a day's work.

Though these companies and their issues have little in common, they do share a technology remedy. It's the Lightweight Directory Access Protocol — or LDAP — a networking protocol that allows end users to more easily navigate the choppy, disparate directories of the rough distributed computing waters.

NationsBank, FedEx and Bay Networks are all in various stages of piloting and implementing LDAP, which they believe will empower users by giving them more control over corporate information.

How so? As an access protocol that comes with a Web browser or mail client, LDAP has opened up possibilities as never before for businesses. Suddenly, end users have the ability to do information lookups, adds and deletes. Administrators can pull information from native application directories into LDAP-based directories and open those up to the corporate intranet, and, by extension, the extranet.

LDAP's popularity stems largely from being a lowest common denominator, according to Doug Simmons, vice president of consulting services at The Radicati Group in Palo Alto, Calif. And though LDAP provides access to disparate data sources, it is limited to name, address and phone number-type information, Simmons points out.

RAPPROCHEMENT

LDAP (a pared-down version of the X.500 access protocol, known as Directory Access Protocol or DAP) has found quick and universal acceptance among traditionally warring competitors. Developed at the University of Michigan, it is easier to implement than DAP, which is very resource-intensive. The functionality provided by LDAP is lighter weight, but Version 3.0 of the protocol has addressed some of the shortcomings by offering, for example, strong authentication.

"THE LDAP MARKET will be impacted by Microsoft's [Active Directory] but not eliminated by Microsoft."

TIM SLOANE, ABERDEEN GROUP

By providing a common interface, LDAP facilitates synchronization of directories across distributed E-mail and other database servers. But while it is popular right now, Microsoft Corp.'s new Active Directory may change the equation, networking experts contend.

And contrary to the claims of LDAP evangelists, the protocol does face other challenges. "LDAP gives us a better opportunity to develop an enterprise directory, but in and of itself does not give an enterprise a consolidated enterprise directory because legacy directories are not based on LDAP," says Gary Rowe, principal at Rapport Communication in Roswell, Ga. "To bring this together, [we need a] new class of products."

In the absence of tools, organizations are developing their own. Ehorn's staff at NationsBank has written custom scripts to extract information from different directories residing on Oracle Corp. and Sybase, Inc. databases distributed throughout the country. The data is then imported into Netscape Communications Corp.'s Directory Server, Version 3.0. In other words, they are aggregating information from multiple sources and putting it into a directory service, which can be used by a certain Web-enabled population.

"The clients of our directory will be a variety of Web applications that require user authentication, or user profile information that may be stored in the directory," Ehorn says.

The use of LDAP will also enable NationsBank to eventually build extranets and leverage the integration of the rest of the Netscape SuiteSpot line, Ehorn says. This approach will "lower the cost of ownership because of centralized administration and [will] decrease development time as applications have one data store about people and groups," he explains.

RATIONALIZING SECURITY

Security is key for Bay Networks, as well. Before June 1997, when Bay saw its first LDAP implementation, the company had a number of security systems, King says. "We had Web developers in each department, each with their own security," he says. "As Web developers sprouted, they created their own security systems."

The result was the creation of as many security systems as applications. Some users could have up to 15 passwords. King said the company is down to about six security systems and the

COVER PHOTOGRAPH BY KURT GERBER

number will go down even more.

King has ambitious expansion plans. For example, he wants to implement digital certificates and use the directory server as a store for public keys. Some applications, such as the New Product Introduction Tool, are extremely sensitive and not all employees on the corporate intranet will have access to them. "It's here that digital certificates will come in handy," King notes.

FedEx, on the other hand, is using LDAP not only for humans to communicate with machines but for intranet applications as well. Although all of its applications are still in beta, FedEx has created a system using software from Entrust Technologies, Inc. in Richardson, Texas.

Employees sign on through Entrust. Each employee gets a certificate that is also stored in the LDAP-based directory. This means that, unlike in the Internet model, a user's certificate does not have to be stored on a particular PC, Candler explains. This does not tie a user to a particular desktop and makes administration a lot easier in an organization where thousands have intranet access.

Once in the directory server, employees have access to "self-service" HR information. Seeker Workplace from Seeker Software, Inc. in Oakland, Calif., provides access to all HR databases, regardless of the platform. Users can change their phone, fax or beeper number, for example, on the HR server.

Salaries and other changes can be made by managers, and all the rules for those are stored in the directory server. In the case of a terminated employee, HR updates the personnel server and all related information across the network is changed at the same time.

The directory server is also the repository for workflow rules. "Our LDAP directory stores workflow enablers — job code, supervisor level, location code, boss, pin number of boss," Candler says. "Client/server applications have access to that data." This means that an application that does expense reports or purchase orders can obtain information, such as who is the signing authority on a particular expense, from the directory server, he explains.

VENDOR BANDWAGON

So while consumers in the business world are rushing to find new ways to use LDAP to bring data within easier reach, vendors are rushing to express their support for LDAP as much through action as through the spoken word.

What vendors like about supporting LDAP is that they each see their product in the center of the directory universe. With a common standard, the focus moves from access to ease of implementation and performance. "As more people write LDAP applications, it takes the spotlight off access and puts it on the back end of the directory," says Michael Simpson, director of product marketing at Novell, Inc. in Provo,

Continued on page 6

Seeking a Master View

A meta directory, says Gary Rowe, principal at Rapport Communication in Roswell, Ga., sits in the middle of disparate directories and lets them communicate with each other. "It understands relationships among various directories, so it can tie them together using an overarching directory structure, like X.500, and weave together various directories," Rowe says.

LDAP could be the protocol used, he contends, because of its universal acceptance.

The chief draw of the meta directory — currently provided by vendors such as Control Data Systems, Inc. in Arden Hills, Minn., and Zoomit Corp. in Toronto, Canada — is that unlike directory synchronization, which merely takes information from different native directories and spits it back out, the meta directory creates a person object into which it puts all the information about that person. It thus does away with the redundancies of traditional directory systems.

Also, unlike X.500, it does not require information to be fully mapped to the native directories, Rowe says.

Tim Sloane, an analyst at Aberdeen Group in Boston, says the meta directory is a concept only partially implemented today, but the concept can be taken to different extremes.

And there will be learning curves to master as people push the meta directory concept a little too far and find that as they try to store too much data in too wide a span of control, management becomes a headache. Then they will have to scale back, he says.

The best use of meta directories, at least with currently available products, is to solve a specific problem, such as managing employee names across applications.

"That's a bold strategy and it can be done," Sloane concludes.

ILLUSTRATIONS BY DAVID BLACK

FOCUS
NUMBER
SERIES
COMPANY
POSITION
NAME

"YOU'VE GOT THE WHOLE WORLD IN YOUR HAND BECAUSE

NET PROFILES

MARK WIESENBERG

052

DIRECTOR, COMPUTER SERVICES

NETWARE
NOVELL DIRECTORY SERVICES

QUALCOMM

DETAILS

E I'VE GOT OUR WHOLE NETWORK ON MY DESKTOP."

Mark Wiesenberg knows all about bringing things down to size.

His company, QUALCOMM, is putting the power of advanced digital wireless communications into the palm of your hand with its compact CDMA digital Q™ phone.

And his network, Novell®, is putting the power of seamless networking right onto his users' desktops. Novell NetWare® software supports over 4,000 users on a single server, and scales up easily as 200 workstations are added every month. And Novell Directory Services™ technology allows his administrators to manage the entire network from a single site (including NT, Mac,® Sun® and UNIX® platforms).

Shrinking the world is hard work, which is why a fast-paced, fast-growing company like QUALCOMM works only with the best. That's why they chose Novell.

World. Network. QUALCOMM. Novell. Hand in hand, desktop to desktop, a revolution in technology.
www.novell.com

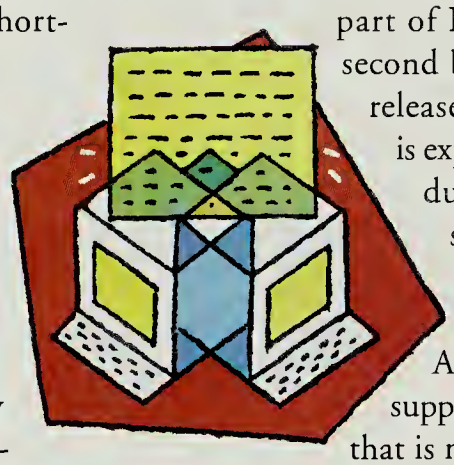
Novell®

SOLUTIONS

Continued from page 3

Utah. "The question then becomes, 'Which [directory] is more reliable, secure and manageable,' " he says.

And all vendors think their products fit the bill. Users and analysts, however, know that LDAP has its shortcomings.



For one, users need to understand the new technology, says Rick Waugh, systems analyst at BCTelecom, Inc. in Vancouver, Canada. You have to figure out the directory schema, what information should be presented to users and what the hierarchy should be. "It doesn't come out of the box ready to go," he says. "It needs design work."

NationsBank's Ehorn recognizes the challenge. Doing schema definition, identifying data sources for schema, providing links to pull existing information into directories, and LDAP-enabling all the applications in use at the bank is time-consuming and can become political as departments squabble over ownership issues.

One area that becomes especially challenging is trying to obtain pieces of information from data repositories, bringing them to the LDAP directory server, and keeping the record keys in the server, Simmons says. The idea is to use the record key to look for additional information on the back-end database.

META DIRECTORIES

A new concept is emerging that defines these directories that manage pointers to other databases. The term "meta directory" came into industry parlance a little more than two years ago. It is used to denote both directories that store pointers as well as one gigantic directory, such as an X.500 directory, that is a repository for all information. Two key features of a meta directory are that it has the intelligence to scan and look for similarities among entries, and it provides centralized management (see story page 3).

Meanwhile, the real challenge to LDAP may come from Microsoft's Active Directory, which will be part of NT Version 5.0, the second beta of which will be released later this year and is expected to become production-ready by the second quarter of next year.

It is true that Active Directory will support LDAP natively but that is not all it will support. On the front end, it will provide the Active Directory Service Interface, which will let independent software vendors write the applications that use the Active Directory; on the back end, Object Linking and Embedding Database or OLE DB — an interface for accessing different types of data regardless of location — will provide access to relational and nonrelational data sources.

For example, "Active Directory will have a ton of new object classes, attributes and object relationships, which are useful only in the NT/Exchange/Wintel environment," Radicati's Simmons says. "These objects have unique names, syntax, object identifiers [and] matching rules, which are not going to be recognizable to non-Active Directory browsers and directories, such as LDAP."

Active Directory may, therefore, limit the proliferation of pure LDAP-based directories that Netscape has been championing. "The LDAP market will be impacted by Microsoft, but not eliminated by Microsoft," says Tim Sloane, an analyst at Aberdeen Group, Inc. in Boston.

Netscape, however, sees meta directories as an interim solution until LDAP becomes more firmly entrenched. "Over the long term, LDAP will make meta directories irrelevant, says Frank Chen, group product manager at Netscape in Mountain View, Calif.

The meta directory issue is a growing one but may not really impress itself on the industry psyche for another two years, industry watchers said.

While some companies will choose something off center and off standard, such as Active Directory, so that they can couple their directories more tightly with their operating system, others will take a different approach, Sloane believes. They will say that the extranet is important to them and they need standards to manage NT and other platforms. And the way to do it will be through LDAP, he contends.

Mohan is a freelance writer in Los Altos, Calif.

Not Lightweight *(to them)*

A SAMPLING OF SERVERS THAT SUPPORT LDAP

LOTUS DEVELOPMENT CORP.
Currently shipping:
Domino Directory, Version 4.61 with LDAP 2.0.
Future release: Version 5.0 with LDAP 3.0

MICROSOFT CORP.
Currently shipping:
NT 4.0. Windows NT Directory Services does not support LDAP.
Future release: NT 5.0 with Active Directory will support LDAP 3.0.

NETSCAPE COMMUNICATIONS CORP.
Currently shipping:
Directory Server, Version 3.0 with LDAP 3.0.

NOVELL, INC.
Currently shipping:
NDS 4.11 with LDAP 2.0.
Future release: NDS 5.0 with LDAP 3.0.

PROJECT: CORPORATE DIRECTORY

And One Directory For All

By Steve Alexander

Parsons Corp., an engineering and construction firm in Pasadena, Calif., will begin using Lightweight Directory Access Protocol (LDAP) as part of a plan to link more than 100 remote small offices and construction sites to its corporate network. An LDAP-based universal corporate directory will initially provide organization charts, employee telephone numbers and personal information. Later the directory will be expanded to include an existing company intranet and a new extranet that will have hundreds of Web pages about individual work projects. Hayes Latin, project manager at systems integrator Perot Systems Corp. explains the project.

WHAT THEY'RE DOING

The LDAP directory will be used to capture data about all the people who need to access information in the organization, including contractors, subcontractors, consultants, partners and employees. We want to categorize users by the organization they are with, the projects they are on and the levels of access they have.

BENEFITS

By having a centralized directory, you put the data in once. When people leave, you can remove them from the central directory and know they have been removed from all applications.

The universal directory also will automate something that has been largely manual. To find someone today, you'd often have to call a building and talk to the guard station. The larger buildings had their own directories, but there was no central directory.

When the corporatewide intranet and extranet are rolled out in six to eight months, they will help the company promote collaboration. People will be able to send documents and drawings back and forth to the remote sites.

HOW THEY'RE DOING IT

Parsons will deploy Oblix, Inc.'s IntraPower Suite 2.5, a tool that allows IS to assign security rights to each field within the LDAP server. Using Oblix, Parsons can say that certain fields are updateable by users, while others are updateable only by company officials. In the future, Parsons will limit the fields to determine what can be viewed by whom. Parsons hasn't decided whether LDAP will run on Windows NT or Unix.

TECHNICAL CHALLENGES

The plan is for any new application in the next three to six months to be LDAP-compliant. But it's questionable whether this will work because some mission-critical applications aren't LDAP-compliant and won't ever be. We may have to maintain separate directories for our homegrown financial system, which runs on an IBM AS/400, and our homegrown materials management system, which runs on an IBM RS/6000. It might be too much of an effort to make those legacy systems work with an LDAP directory.

The company must figure out how to replicate the directory database to other servers in the network.

WHAT'S ONLINE

For an expanded view of this project with RealAudio clips, point your browser to
www.computerworld.com/intranets

TOOLS

In addition to IntraPower, Netscape Directory 3.0 is the directory server.

COSTS

The LDAP directory and the Oblix interface were justified by the universal corporate directory function. IS was sold on the network security and application security aspects.

RETURN ON INVESTMENT

Management justified the expenditure on the convenience and utility of LDAP.

ADVICE TO OTHERS

It might be too cumbersome to rework legacy applications to fit the LDAP model. But if you shift to Web-based applications, you need to be concerned about security. That's where LDAP is of value.

"By having a centralized directory, you put the data in once. When people leave, you can remove them from the central directory and they have been removed from all applications."

HAYES LATIN
Project Manager
Perot Systems Corp.

PHOTO BY GARY MOSS

Alexander is a freelance writer in Edina, Minn.

COMPUTERWORLD INTRANETS *is published monthly on the fourth Monday of the month as a supplement to Computerworld. Editor: Alan Alper; Designer: Mary Beth Welch; Assistant Managing Editor: Kimberlee A. Smith; Copy Editor: Catherine McCrorey; Computerworld Magazines Editor: Alan Alper. Phone: (800) 343-6474; E-mail: alan_alper@cw.com.*

EVER WONDER WHICH NETWORKING COMPANY THE EXPERTS RECOMMEND?

- "AWARD OF DISTINCTION," EDITOR'S CHOICE, *BYTE* MAGAZINE — NETWARE®
- "HIGHEST IN CUSTOMER SATISFACTION," *COMPUTERWORLD* BUYERS GUIDE SURVEY
- "PRODUCT OF THE YEAR, BEST NOS," *INFOWORLD*
- "NOVELL'S THE ONE," *INFOWORLD*
- "PRODUCT OF THE YEAR, BEST NOS," *LAN* MAGAZINE
- "WELL-CONNECTED AWARD, BEST NOS," *NETWORK COMPUTING*
- "PRODUCT OF THE YEAR, SERVER OPERATING SYSTEMS," *NETWORK* MAGAZINE
- "HIGHEST IN CUSTOMER SATISFACTION," *COMPUTERWORLD* BUYERS GUIDE SURVEY — GROUPWISE®
- "HIGHEST IN SOFTWARE QUALITY," *COMPUTERWORLD* BUYERS GUIDE SURVEY
- "PRODUCT OF THE YEAR, E-MAIL/MESSAGING," *LAN* MAGAZINE
- "WELL-CONNECTED AWARD, BEST CLIENT/SERVER MESSAGING," *NETWORK COMPUTING*
- "WELL-CONNECTED AWARD, BEST DIRECTORY," *NETWORK COMPUTING* — NOVELL DIRECTORY SERVICES™
- "PRODUCT OF THE YEAR, SYSTEMS MANAGEMENT," *NETWORK* MAGAZINE — MANAGEWISE®

Novell®

HONORS

All awards were received in 1997.